Craig Spencer - Unit 4 Homework

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.

   - Command to inspect permissions:

```
ls -l shadow gshadow group passwd

-rw-r--r-- 1 root root   1303 May 14 16:31 group

-rw-r----- 1 root shadow 1076 May 14 16:31 gshadow

-rw-r--r-- 1 root root   3214 May 14 16:31 passwd

-rw-r----- 1 root shadow 2888 May 14 16:31 shadow
```

   - Command to set permissions (if needed):

2.

Permissions on `/etc/shadow` should allow only `root` read and write access.

```
sudo chmod 600 shadow

ls -l | grep shadow

-rw------- 1 root shadow 2888 May 14 16:31 shadow
```

Permissions on `/etc/gshadow` should allow only `root` read and write access.

```
sudo chmod 600 gshadow

ls -l | grep gshadow

-rw------- 1 root gshadow 1076 May 14 16:31 gshadow
```

Permissions on `/etc/group` should allow `root` read and `write` access, and allow everyone else `read` access only.

Does not require changing but command would be for group and group files:

sudo chmod 644 group passwd

-rw-r--r-- 1 root root   1303 May 14 16:31 group

-rw-r--r-- 1 root root   3214 May 14 16:31 passwd

Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin.

   - ○ Command to add each user account (include all five users):

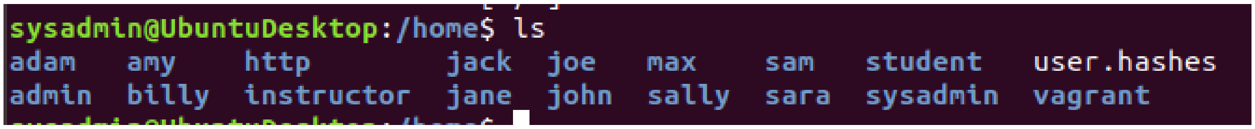
sudo adduser sam

sudo adduser joe

sudo adduser amy

sudo adduser sara

sudo adduser admin



```
sysadmin@UbuntuDesktop:/home$ ls
adam   amy    http         jack  joe   max    sam   student   user.hashes
admin  billy  instructor   jane  john  sally  sara  sysadmin  vagrant
```

2. Ensure that only the admin has general sudo access.

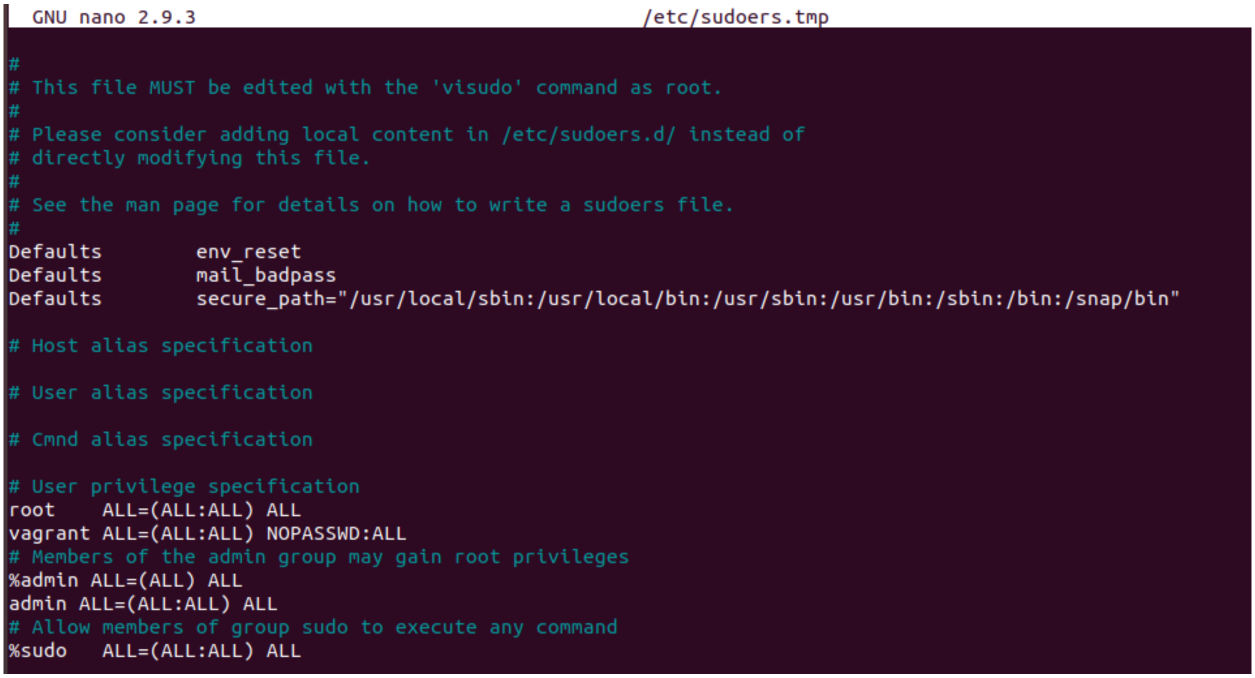
   - ○ Command to add admin to the sudo group:

sudo usermod -aG sudo admin

sysadmin@UbuntuDesktop:~$ id admin

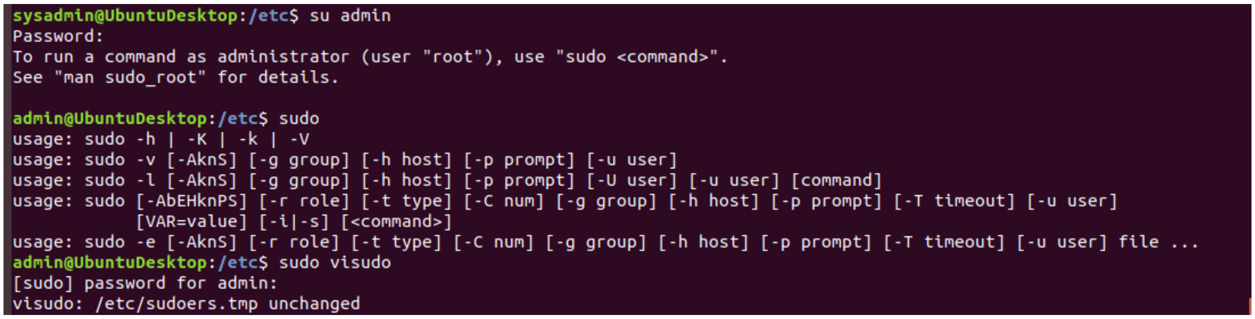
uid=1016(admin) gid=1018(admin) groups=1018(admin),**27(sudo)**

- ○ Add Admin to sudoers list **sudo visudo**
- ○ **See below screen shot**

○ 

```
  GNU nano 2.9.3                                    /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
vagrant ALL=(ALL:ALL) NOPASSWD:ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
admin ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

Check by su to admin and run sudo It worked!:



```
sysadmin@UbuntuDesktop:/etc$ su admin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@UbuntuDesktop:/etc$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
admin@UbuntuDesktop:/etc$ sudo visudo
[sudo] password for admin:
visudo: /etc/sudoers.tmp unchanged
```

Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.

    - Command to add group:
    - sudo groupadd -g 1019 engineers (had to find next GID from passwd file)

2. Add users sam, joe, amy, and sara to the managed group.

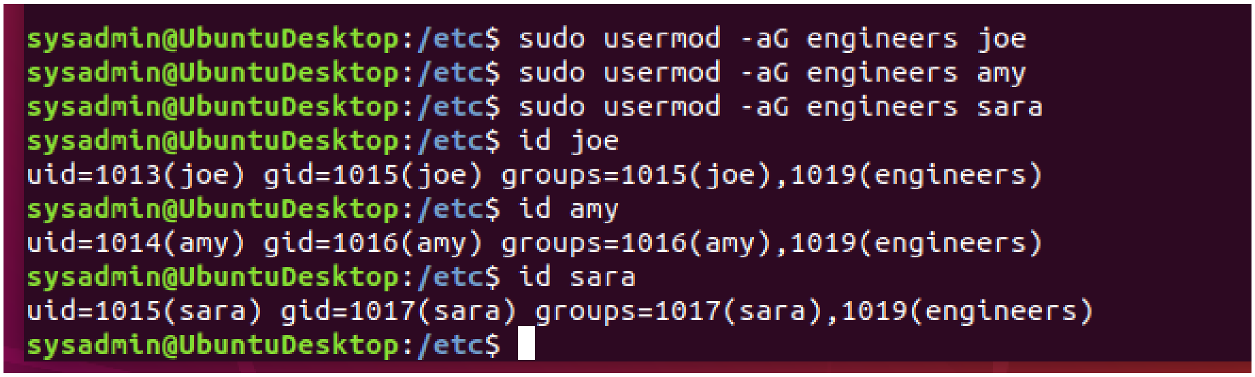
- Command to add users to engineers group (include all four users):

sudo usermod -aG engineers sam

sysadmin@UbuntuDesktop:/etc$ id sam

uid=1012(sam) gid=1014(sam) groups=1014(sam),1019(engineers)

Run for other users and confirm with ID: see for remaining users

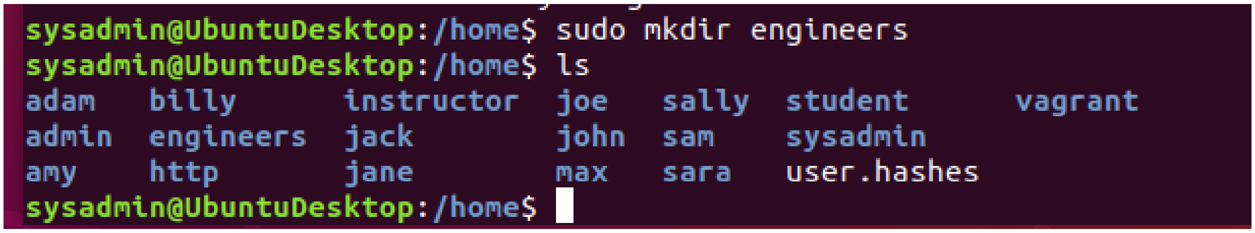


```
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers joe
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers amy
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers sara
sysadmin@UbuntuDesktop:/etc$ id joe
uid=1013(joe) gid=1015(joe) groups=1015(joe),1019(engineers)
sysadmin@UbuntuDesktop:/etc$ id amy
uid=1014(amy) gid=1016(amy) groups=1016(amy),1019(engineers)
sysadmin@UbuntuDesktop:/etc$ id sara
uid=1015(sara) gid=1017(sara) groups=1017(sara),1019(engineers)
sysadmin@UbuntuDesktop:/etc$
```

3. Create a shared folder for this group at /home/engineers.

   - Command to create the shared folder:

     sudo mkdir engineers in home directory



```
sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers
sysadmin@UbuntuDesktop:/home$ ls
adam   billy      instructor  joe   sally  student      vagrant
admin  engineers  jack        john  sam    sysadmin
amy    http       jane        max   sara   user.hashes
sysadmin@UbuntuDesktop:/home$
```

4. Change ownership on the new engineers' shared folder to the engineers group.

   - Command to change ownership of engineer's shared folder to engineer group:

sudo chown root:engineers engineers

sysadmin@UbuntuDesktop:/home$ ls -l

total 76

drwxr-xr-x 8 adam   adam   4096 May 14 16:29 adam

```
drwxr-xr-x  9 admin      admin      4096 Sep 18 07:14 admin

drwxr-xr-x  8 amy        amy        4096 Sep 18 03:48 amy

drwxr-xr-x  8 billy      billy      4096 May 14 16:29 billy

drwxr--rwx  2 root       engineers  4096 Sep 18 07:37 engineers

drwxr-xr-x  8 http       http       4096 May 14 16:29 http

drwxr-xr-x  9 instructor instructor 4096 May 14 16:36 instructor

drwxr-xr-x  8 jack       jack       4096 May 14 16:29 jack

drwxr-xr-x  8 jane       jane       4096 May 14 16:31 jane

drwxr-xr-x  8 joe        joe        4096 Sep 18 03:47 joe

drwxr-xr-x  8 john       john       4096 May 14 16:29 john

drwxr-xr-x  8 max        max        4096 May 14 16:29 max

drwxr-xr-x  8 sally      sally      4096 May 14 16:29 sally

drwxr-xr-x  8 sam        sam        4096 Sep 18 03:46 sam

drwxr-xr-x  8 sara       sara       4096 Sep 18 03:48 sara

drwxr-xr-x  8 student    student    4096 May 14 16:24 student

drwxr-xr-x 17 sysadmin   sysadmin   4096 Sep 18 07:16 sysadmin

-rw-r--r--  1 root       root       1581 May 14 16:29 user.hashes

drwxr-xr-x 10 vagrant    vagrant    4096 May 14 16:41 vagrant

sudo chmod 774  engineers

ls -l

drwxrwxr--  2 root       engineers  4096 Sep 18 07:37 engineers
```

Root and engineer have read, write, and execute permissions others have read only

Step 4: Lynis Auditing

1. Command to install Lynis:

   sudo apt install lynis

2. Command to see documentation and instructions:

   Man lynis

3. Command to run an audit:

   Sudo lynis audit system --logfile/lynis.log

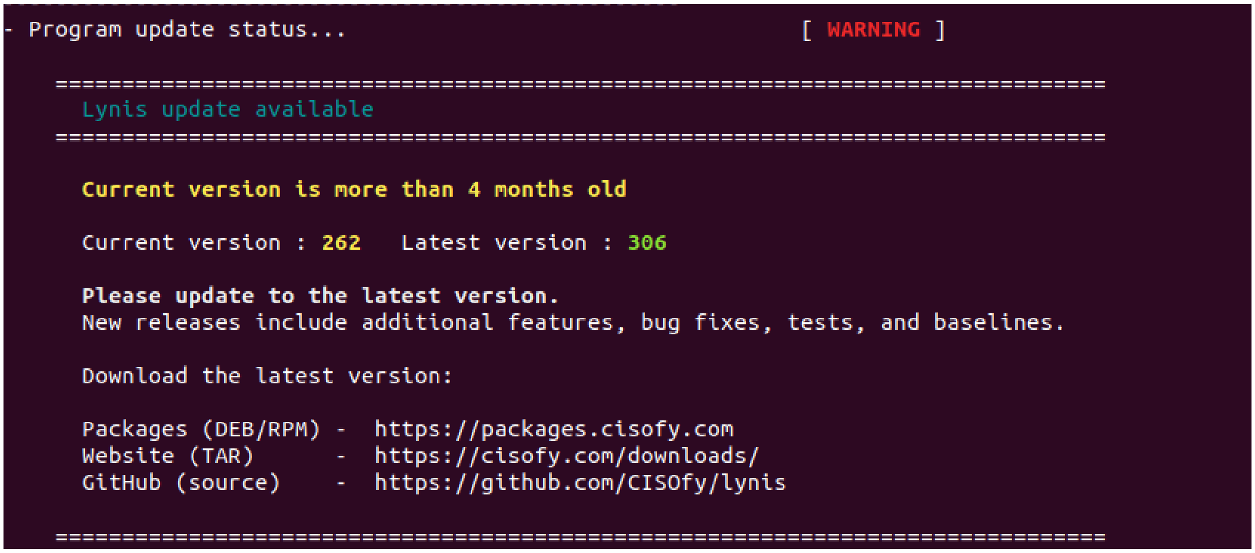
   Or

   Sudo lynis audit system --quick

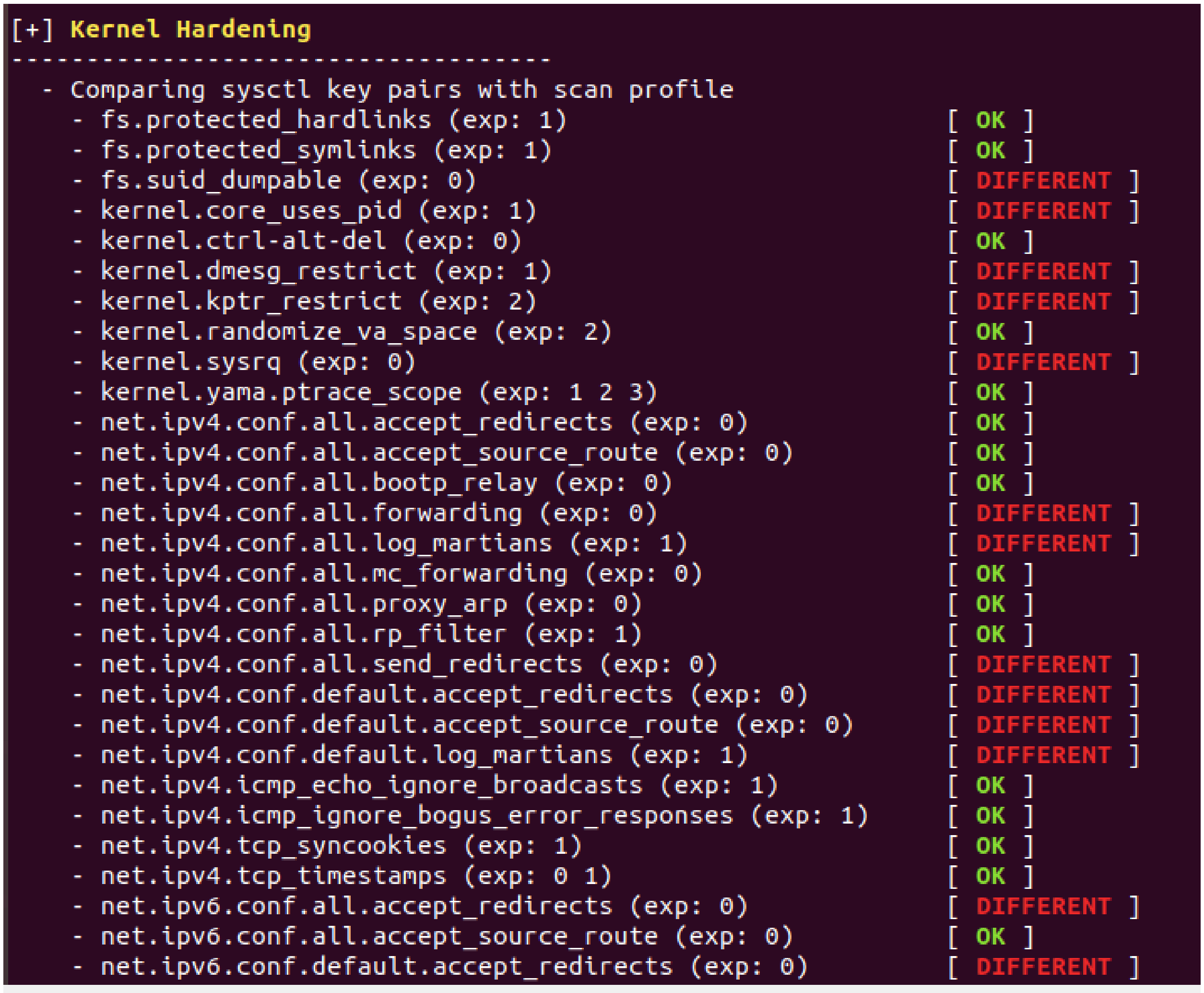
4. Provide a report from the Lynis output on what can be done to harden the system.

   ○ Screenshot of report output:

   Update lynis warning:



```
- Program update status...                                   [ WARNING ]

    ===============================================================================
      Lynis update available
    ===============================================================================

      Current version is more than 4 months old

      Current version : 262   Latest version : 306

      Please update to the latest version.
      New releases include additional features, bug fixes, tests, and baselines.

      Download the latest version:

      Packages (DEB/RPM) -  https://packages.cisofy.com
      Website (TAR)      -  https://cisofy.com/downloads/
      GitHub (source)    -  https://github.com/CISOfy/lynis

    ===============================================================================
```



```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - fs.protected_hardlinks (exp: 1)                         [ OK ]
    - fs.protected_symlinks (exp: 1)                          [ OK ]
    - fs.suid_dumpable (exp: 0)                               [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                           [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                            [ OK ]
    - kernel.dmesg_restrict (exp: 1)                          [ DIFFERENT ]
    - kernel.kptr_restrict (exp: 2)                           [ DIFFERENT ]
    - kernel.randomize_va_space (exp: 2)                      [ OK ]
    - kernel.sysrq (exp: 0)                                   [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                   [ OK ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)             [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                   [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)                 [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                    [ OK ]
    - net.ipv4.conf.all.send_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)      [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)             [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)           [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)     [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                        [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                      [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
```

Warnings (4):

! Version of Lynis is very old and should be updated [LYNIS]

https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]

https://cisofy.com/controls/AUTH-9308/

```
  ! Found one or more vulnerable packages. [PKGS-7392]

      https://cisofy.com/controls/PKGS-7392/


  ! Found some information disclosure in SMTP banner (OS or software name)
[MAIL-8818]

      https://cisofy.com/controls/MAIL-8818/


  Suggestions (53):

  ----------------------------

  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]

      https://your-domain.example.org/controls/CUST-0280/


  * Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]

      https://your-domain.example.org/controls/CUST-0285/


  * Install apt-listbugs to display a list of critical bugs prior to each APT installation.
[CUST-0810]

      https://your-domain.example.org/controls/CUST-0810/


  * Install apt-listchanges to display any significant changes prior to any upgrade via APT.
[CUST-0811]

      https://your-domain.example.org/controls/CUST-0811/


  * Install debian-goodies so that you can run checkrestart after upgrades to determine
which services are using old versions of libraries and need restarting. [CUST-0830]

      https://your-domain.example.org/controls/CUST-0830/
```

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]

https://your-domain.example.org/controls/CUST-0831/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]

https://your-domain.example.org/controls/CUST-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]

https://your-domain.example.org/controls/CUST-0875/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

https://cisofy.com/controls/DEB-0880/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

https://cisofy.com/controls/BOOT-5122/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]

https://cisofy.com/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/controls/AUTH-9286/

```
  * Configure maximum password age in /etc/login.defs [AUTH-9286]

      https://cisofy.com/controls/AUTH-9286/


  * Set password for single user mode to minimize physical access attack surface [AUTH-9308]

      https://cisofy.com/controls/AUTH-9308/


  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

      https://cisofy.com/controls/AUTH-9328/


  * To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]

      https://cisofy.com/controls/FILE-6310/


  * To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]

      https://cisofy.com/controls/FILE-6310/


  * To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]

      https://cisofy.com/controls/FILE-6310/


  * Check 8 files in /tmp which are older than 90 days [FILE-6354]

      https://cisofy.com/controls/FILE-6354/
  * Disable drivers like USB storage when not used, to prevent unauthorized storage or
data theft [STRG-1840]

      https://cisofy.com/controls/STRG-1840/


  * Check DNS configuration for the dns domain name [NAME-4028]

      https://cisofy.com/controls/NAME-4028/


  * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command.
This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]

      https://cisofy.com/controls/PKGS-7346/


  * Install debsums utility for the verification of packages with known good database.
[PKGS-7370]

      https://cisofy.com/controls/PKGS-7370/


  * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or
unattended-upgrades [PKGS-7392]

      https://cisofy.com/controls/PKGS-7392/


  * Install package apt-show-versions for patch management purposes [PKGS-7394]

      https://cisofy.com/controls/PKGS-7394/


  * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]

      https://cisofy.com/controls/NETW-3032/


  * Access to CUPS configuration could be more strict. [PRNT-2307]
```

```
      https://cisofy.com/controls/PRNT-2307/


  * You are advised to hide the mail_name (option: smtpd_banner) from your postfix
configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf)
[MAIL-8818]

      https://cisofy.com/controls/MAIL-8818/


  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]

    - Details  : disable_vrfy_command=no

    - Solution : run postconf -e disable_vrfy_command=yes to change the value

      https://cisofy.com/controls/MAIL-8820/


  * Check iptables rules to see which rules are currently not used [FIRE-4513]

      https://cisofy.com/controls/FIRE-4513/


  * Install Apache mod_evasive to guard webserver against DoS/brute force attempts
[HTTP-6640]

      https://cisofy.com/controls/HTTP-6640/


  * Install Apache modsecurity to guard webserver against web application attacks
[HTTP-6643]

      https://cisofy.com/controls/HTTP-6643/


  * Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and
privacy [HTTP-6710]

      https://cisofy.com/controls/HTTP-6710/
```

```
* Consider hardening SSH configuration [SSH-7408]
  - Details  : AllowTcpForwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : ClientAliveCountMax (3 --> 2)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : Compression (YES --> (DELAYED|NO))
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : LogLevel (INFO --> VERBOSE)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : MaxAuthTries (6 --> 2)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : MaxSessions (10 --> 2)
    https://cisofy.com/controls/SSH-7408/
```

```
* Consider hardening SSH configuration [SSH-7408]
  - Details  : PermitRootLogin (WITHOUT-PASSWORD --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : Port (22 --> )
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : TCPKeepAlive (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : X11Forwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : AllowAgentForwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Check what deleted files are still in use and why. [LOGG-2190]
    https://cisofy.com/controls/LOGG-2190/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
```

```
      https://cisofy.com/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/controls/ACCT-9622/

  * Enable sysstat to collect accounting (no results) [ACCT-9626]
      https://cisofy.com/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/controls/ACCT-9628/

  * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
      https://cisofy.com/controls/CONT-8104/

  * One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
    - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
      https://cisofy.com/controls/KRNL-6000/

  * Harden compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/controls/HRDN-7222/
```

Bonus

1. Command to install chkrootkit:

   sudo apt install chkrootkit

2. Command to see documentation and instructions:

   Man chkrootkit

3. Command to run expert mode:

   Sudo chkrootkit -x

4. Provide a report from the chkrootkit output on what can be done to harden the system.

I found that the expert mode did not seem to pick up the infected vulnerabilities like the quiet and normal mode did. It may be the infection is a false positive but I would still investigate "INFECTED: Possible Malicious Linux.Xor.DDoS installed"

```
sysadmin@UbuntuDesktop:/usr/sbin$ sudo chkrootkit
```

(Sample)

```
ROOTDIR is `/'

Checking `amd'...                                  not found

Checking `basename'...                               not infected

Checking `biff'...                                 not found

Checking `chfn'...                                 not infected

Searching for Malicious TinyDNS ...                   nothing found

Searching for Linux.Xor.DDoS ...                     INFECTED: Possible Malicious
Linux.Xor.DDoS installed

/tmp/burpsuite_community_linux_v2020_11_3.sh
```

```
/tmp/rev_shell.sh

/tmp/vagrant-shell

/tmp/response.varfile

/tmp/lynis.log

/tmp/a9xk.sh

/tmp/listen.sh

Checking `OSX_RSPLUG'...
```

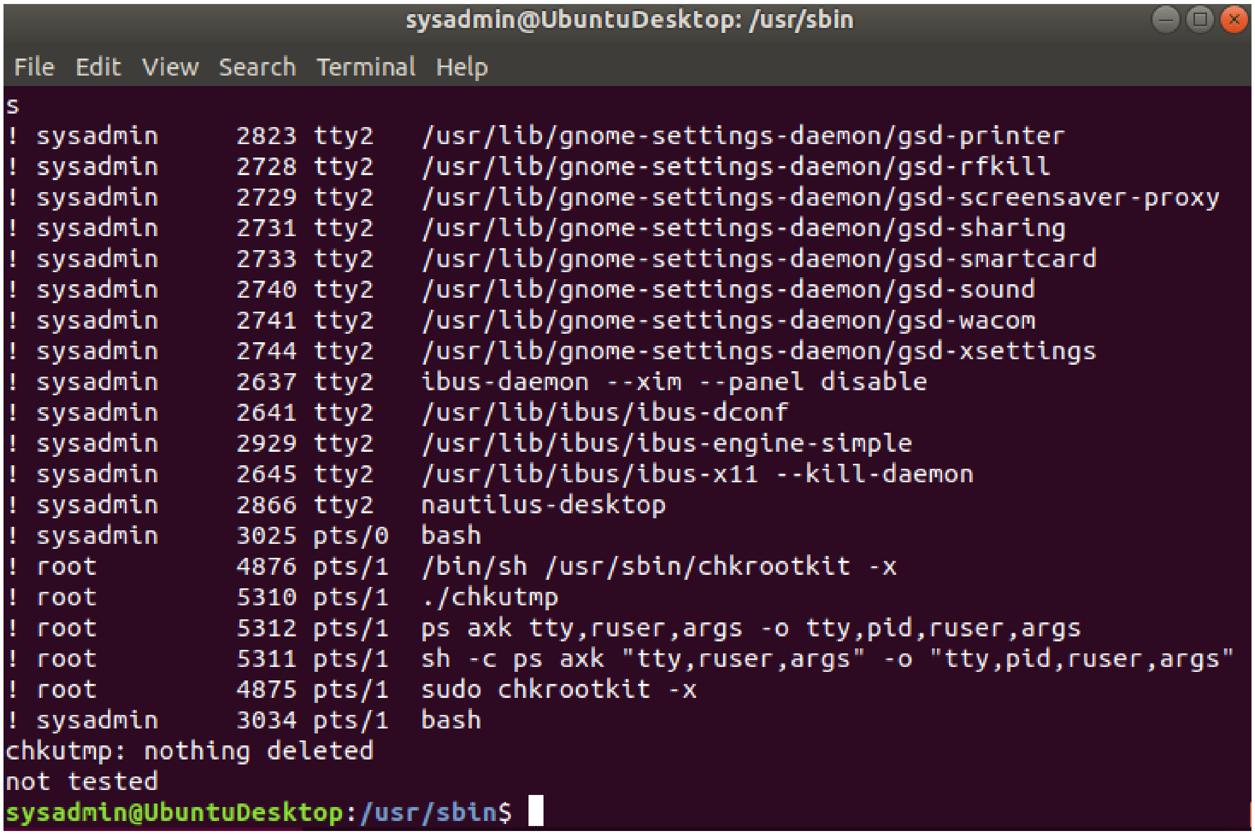
Show only suspicious in quiet mode:

```
sudo chkrootkit -q
```

```
/usr/lib/debug/.build-id
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/files/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/.travis.yml
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/templates/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/roles/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/files/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/.travis.yml
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/templates/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/files/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/.travis.yml
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/templates/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/files/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/.travis.yml
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/templates/.git_keep
/lib/modules/5.0.0-23-generic/vdso/.build-id

/usr/lib/debug/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id

not tested

INFECTED: Possible Malicious Linux.Xor.DDoS installed
```

- Screenshot of end of sample output:

Sudu chkrootkit -x



sysadmin@UbuntuDesktop: /usr/sbin
File Edit View Search Terminal Help

```
s
! sysadmin     2823 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2728 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2729 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2731 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2733 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2740 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2741 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2744 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2637 tty2   ibus-daemon --xim --panel disable
! sysadmin     2641 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2929 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2645 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2866 tty2   nautilus-desktop
! sysadmin     3025 pts/0  bash
! root         4876 pts/1  /bin/sh /usr/sbin/chkrootkit -x
! root         5310 pts/1  ./chkutmp
! root         5312 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root         5311 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         4875 pts/1  sudo chkrootkit -x
! sysadmin     3034 pts/1  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/usr/sbin$ 
```